

# **EXHIBIT 13**



# Annual Financial Statements and Management Report of Deutsche Bank AG 2017



# Content

## 1 — Management Report

3	Operating and Financial Review
15	Outlook
21	Risks and Opportunities
25	Risk Report
51	Compensation Report
93	Internal Control over Financial Reporting
96	Non-financial Statement
115	Information pursuant to Section 289(4) of the German Commercial Code and Explanatory Report
119	1a—Appendix to the Management Report: Report on equal treatment and equal pay

---

## 2 — Annual Financial Statement

122	Balance Sheet as of December 31, 2017
124	Income Statement for the period from January 1 to December 31, 2017
125	Notes to the Accounts

---

## 3 — Confirmations

180	Responsibility Statement by the Management Board
181	Independent Auditor's Report

---

**PAGES 2-105 OMITTED  
PURSUANT TO D. N.J. ECF  
POLICIES AND  
PROCEDURES**

## Anti-Financial Crime

As a responsible bank, we view how we conduct our business as at least as important as our financial performance. We have a long history of supporting regulations and procedures at international level to combat financial crime and we consider this as vital to ensuring the stability of banks and the integrity of the international financial system as a whole. This helps to protect the bank from being misused for committing criminal offences. Besides that, ignoring financial crime provisions potentially exposes us to corporate criminal and/or regulatory liability, civil lawsuits and a loss of reputation.

AFC policies are at least reviewed annually to ensure that new regulation is properly reflected in the policies.

Ultimate responsibility for AFC lies with our Management Board, while our AFC division is tasked with the day-to-day prevention of money laundering and terrorism financing, adhering to sanctions' and embargo' regimes, and preventing fraud, bribery and corruption or any other criminal activity. A key objective in 2017 was to strengthen the AFC division, therefore the department has increased the number of staff by 60 % during the year.

The AFC organization is subdivided into Regional, Global and Central Functions. Their main responsibility is described as follows:

- Regional Functions take responsibility for the regions Deutsche Bank is operating in (Germany, Americas, UK and Ireland, Asia Pacific/APAC, and Europe, Middle East and Africa/EMEA).
- Global Functions manage Anti-Money Laundering (AML)/Terrorism Financing, Sanctions & Embargoes and Anti-Fraud, Bribery and Corruption
- Central Functions manage topics like Risk & Controls, Investigations as well as Regulatory Governance & Enforcement

Without prejudice to the Management Board's oversight duty and the delegation of the above mentioned tasks to the AFC organization, ultimate accountability for the appropriate structuring and execution of transactions/business activities and their corresponding processes lies with the line managers and employees in the respective business divisions.

Every employee must carefully familiarize themselves and keep up to date with applicable policies and regulations to comply with them.

## Employee Training and Engagement

We deliver training to help employees understand regulation, compliance, and AFC. There are a range of courses available depending on audience type (this section does apply to AFC organization).

### Graduates

- Graduate induction week for new joiners in AFC or Compliance departments;
- Dedicated training sessions for graduates in all divisions highlighting the importance of managing AFC and Conduct Risk

### AFC/Compliance Employees

- “First 100 days” induction process;
- Various technical development programs on topics such as “how to conduct an internal investigation”

### Bank Employees

There is a group-wide AFC curriculum on courses covering AML, Fraud Awareness, Anti-Bribery and Corruption and Sanctions. Uptake of these courses is very high with very low overdue ratios for late or non-completion.

## AFC Risk & Control

The Global AFC Risk & Controls Team together with other AFC functions and business divisions or infrastructure functions assesses and identifies risks of money laundering and terrorism financing, sanctions and embargoes, fraud, bribery and corruption, resulting from our products, services and client activities. In order to meet these targets, clients, products and transactions are assessed annually through the Global AFC risk assessment as well as quarterly via Top Risk reporting which is a group-wide process and part of our non-financial risk framework. Assessments are continuously enhanced and reviewed to adjust them to the new regulatory requirements.

The Global AFC Risk & Controls Team sets the framework and provides the technical platform for assessments that are conducted on country or legal entity levels.

The key objectives of the risk assessment are to better understand the risks inherent in our products and services, client activities and the geographic locations we operate in.

## Know Your Client, KYC

The bank's Know Your Client (KYC) Policy sets the rules that govern our group-wide approach to KYC. In conducting KYC, we seek to comply with all relevant national and international laws and regulations. In 2017, the bank implemented a new KYC program that applies to every country we operate in, paying special attention to high-risk clients (such as politically exposed persons, PEP), promoting greater business accountability, providing clearer guidance and application, as well as embedding and raising awareness of the bank's risk appetite thresholds.

Clients are assessed as part of due diligence and are regularly screened against internal and external criteria. In 2017, we continued to roll out an extended screening program, which serves as the basis for further enhancement with regards to screening effectiveness and efficiency.

As a consequence of due diligence, a client relationship may be declined or subject to monitoring or conditions imposed on accounts, transactions, or product usage. In cases of suspicious activity, regulatory and government bodies are informed according to existing legal and regulatory requirements.

KYC is an ongoing process throughout the lifecycle of the client relationship. As such, we must know not only the client but also the anticipated nature of the client relationship.

The New Client Adoption process deals with the on-boarding of potential clients. No funds or assets may be accepted or transacted, nor any legal commitment entered into (including the operation of an account, sale of a product, or rendering of a service) prior to fully completed adoption of the client.

In order to periodically assess client relationships, the business must ensure that regular reviews of all existing clients are initiated and duly performed. Review cycles depend on the risk category of a client relationship. In general, high risk clients must be reviewed annually, medium risk clients every two years and low risk clients every five years.

Assessing and understanding client-related money laundering and terrorist financing risks is a critical component of our AFC Risk Management framework, which helps us mitigate and manage risk in line with our financial crime risk appetite.

The primary objective of risk segmenting our client base is to conduct appropriate due diligence and to ensure a comprehensive client profile is in place to enable the comparison of the results of ongoing monitoring and identify any discrepancies.

Our risk rating methodology considers the following aspects of each client relationship to determine a Client Risk Rating: Country Risk, Industry Risk, Product Risk and Entity Type Risk. Irrespective of the risk type, if the client is a politically exposed person (PEP) or an ultimate beneficial owner of the client is a PEP, they will always be classified as high risk.

## Anti-Money Laundering and Terrorism Financing

Within our AFC function the AML unit is responsible for instituting measures to prevent money laundering and combat the financing of terrorism, including measures to

- comply with rules and regulations regarding identification (authentication), recording and archiving;
- detect suspicious transactions and process suspicious activity alerts; and
- develop, update and execute internal policies, procedures and controls.

Irrespective of the value or amount, if there is a reasonable suspicion that funds have been derived from illegal origins or may be used in the context of terrorism financing, the transaction must be declined.

The AML unit is designed to comply with German rules as a minimum, as well as local laws and regulations in all countries the bank operates in. It includes policies, procedures, a designated Money Laundering Officer, independent controls and regular employee training. The percentage of overdue AML trainings is 0.08 %.

We are part of the Wolfsberg Group of Banks and have adopted the Wolfsberg Anti-Money Laundering Principles, as well as signing the Wolfsberg Statement on the Suppression of the Financing of Terrorism.

## Respecting Sanctions and Embargoes

National authorities and supranational organizations (such as United Nations (UN), European Union (EU)) impose restrictive measures against countries, organizations, groups, entities and individuals that infringe internationally accepted behaviors and norms, especially where these relate to weapons proliferation, terrorism or support of terrorist organizations, human rights violations, or corruption and bribery. Such measures are more commonly known as embargoes or sanctions.

Deutsche Bank has a responsibility to monitor, evaluate, and, if required, observe laws and binding requirements related to financial and trade sanctions set by the EU, Bundesbank, Germany's Federal Office for Economic Affairs and Export Control, and other authorities, such as the US Office of Foreign Assets Control (OFAC) and the UK Treasury Department.

Our group-wide Embargo Policy, Special Risk Country Policy, and a specific Office of Foreign Assets Control Policy help us assess and reduce client risk as part of our on-boarding processes and periodically thereafter. It also helps us manage risks related to particular transactions, countries, and goods.

In the wake of the implementation of the Joint Comprehensive Plan of Action entered into by world powers and Iran at the start of 2016, we have very cautiously relaxed our otherwise stringent policy towards Iran, and in 2017, we continued to execute legal payments on behalf of our long-standing clients in Euros, subject to enhanced due diligence.

## Combating Bribery and Corruption

Bribery and Corruption risks can arise in our daily operations. Bribery means improperly offering, promising, giving, authorizing, soliciting, agreeing to receive or accepting anything of value to or from another person or entity. Corruption means any activity that involves the abuse of position or power for an improper personal or business advantage, whether in the public or private sector.

Deutsche Bank takes a zero-tolerance approach to bribery and corruption, in line with its Code of Business Conduct and Ethics, values and beliefs, and international law, including the UK Bribery Act 2010, the US Foreign Corrupt Practices Act 1977, the German Criminal Code, and the OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions.

Reflecting our commitment to comply with applicable law and regulations, as well as best practice standards, our Anti-Fraud, Bribery and Corruption (AFBC) unit is responsible for:

- monitoring and advising on compliance related to bribery and corruption laws, regulations and international standards;
- the ongoing design and development of appropriate measures to mitigate bribery and corruption risk;
- administering controls and safeguards to mitigate bribery and corruption risk.

The ABC Policy sets out the minimum standards of behavior expected by all employees and third parties associated with Deutsche Bank (including partners, suppliers, service providers and Third Parties, to the extent they perform services to the Group, subject to contractual agreements).

Staff reliability checks are conducted for all new hires. A updated reliability check process for existing employees has been rolled out during 2017.

Every employee is responsible for the prevention, detection and reporting of bribery and other forms of corruption in connection with our business. Bribery and corruption have serious consequences for employees and the bank. An employee who gives, receives or agrees to give or receive a bribe violates the ABC Policy, the Code of Business Conduct and Ethics and is committing a criminal and/or regulatory offence potentially exposing us to corporate criminal and/or regulatory liability and civil lawsuits locally and globally. The employee may also be subjected to civil or criminal fines and penalties and/or imprisonment. Senior Management can be prosecuted and may be personally liable if they become aware that an act of bribery has taken place, or will take place, and do not take appropriate action to prevent it. Equally, we may terminate relationships with any third party found to be in breach of the principles and rules set out in the ABC Policy or applicable bribery and corruption laws and regulations.

To deliver the policy, regional teams are responsible for analyzing risk, developing and monitoring controls, training, and awareness.

## Information Security

Clients expect to access the services they need anytime, anywhere, and through a variety of channels. Evolving and innovating our technology, service offering and processes in many instances builds on partnering with service providers and the integration of Fintech development. In parallel, cyber-attacks on businesses are increasing in scale, speed, and sophistication. Information Security therefore is one of Deutsche Bank's material non-financial topics. Preserving the confidentiality, integrity and availability of our clients' & partners' data and the bank's information assets is essential for upholding the trust placed in Deutsche Bank by our clients, shareholders, employees and other stakeholders.

## Governance

Our governance framework and cyber security program are continuously enhanced to ensure that security policies and standards continue to mirror evolving business requirements, regulatory guidance, and emerging cyber threats. Information security policies support Deutsche Bank in complying with these parameters and build the foundation for actively managing and governing information security related implementation processes. International standards and best practices are used to structure Deutsche Bank's comprehensive information security policy landscape. Our information Security Management System is certified to the international ISO 27001 standard since 2012 and was re-certified in 2015. Our policies provide a formal declaration of the Management Board's commitment to ensuring the security of the bank's information. A decision-making "IT Security Committee" with delegated authority from the COO representative of the management board is furthermore well established to oversee all activities including potential escalations.

**PAGES 110-192 OMITTED  
PURSUANT TO D. N.J. ECF  
POLICIES AND  
PROCEDURES**